TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 15, No. 1, July 2015, pp. 184 ~ 190
DOI: 10.11591/telkomnika.v15i1. 8088

KAMAN Protocol for Preventing Virtual Side Channel Attacks in Cloud Environment

Hardeep Kaur*, Manjit Kaur
Department of Computer Science Engineering Lovely Professional University Jalandhar, Punjab, India
*Corresponding author, email: hardeepkaurkahlon@yahoo.in

Abstract

Now a day cloud computing is widely accepted all around the world used for public utilities and on demand computing services. It provides lots of benefits like storage, easy access to system anytime, broad network access, resource pooling etc. Various attacks can be performed by attackers or intruder due to its large emergence. In these days security and privacy of user's data is main concern. An attacker can access and analyse the data of users by penetrating in the cloud by different approaches. An unintelligent cloud service provider or cloud resource management can significantly increases the leakage of the information of the users. In this paper, a virtual side channel attack is described where attacker hijacks all the credential of authorized user and access user's data. A proposed solution is provided to isolate the attack.

Keywords: *cloud computing, virtual machine, virtual side channel attack, KAMAN protocol*

1. Introduction

Background: Cloud computing is a biggest scale paradigm which receives a significant attention recently. Cloud computing provides their customers different types of services like software services, platform services, infrastructure services. Software as a service (SaaS) provides the facility to use the application on cloud without installing it on their own computer. Platform as a service (PaaS) provides the customers the platform where they can run the applications and develop the application through different programming languages. Infrastructure as a service (IaaS) provides customers the storage and computing facilities [1, 4]. Resources are managed and pooled together for balancing the workload properly and for their efficient access. Amazon web services, Google app engine, Window azure, Sales force.com etc. provides these various services to their users [2]. The main three models which are deployed in cloud computing are: public cloud, private cloud, hybrid cloud. Public cloud is accessible by everyone as cloud provider makes resources (storage and application etc.) available to general public through internet. Private Cloud infrastructure is handles by third party and operated for single organisation. Hybrid cloud is combination of private and public cloud [6, 7]. The main attributes of cloud computing are multi-tenancy, scalability, elasticity, resource pooling, pay as you go [3].

Problem: As security is the main concern in cloud computing various types of attacks are possible which violates the privacy and integrity of user's data on cloud. Virtual side channel attack is possible in cloud environment where an attacker replace his virtual machine with cloud virtual machine and forces a user to give his credential to attackers. When attacker hijack all the credential of a legitimate user, attacker access the cloud services as an legitimate user and authenticate as valid authorized user and can access to user's data [5].

Proposed Solution: To isolate this attack, an approach which is proposed in this paper is to authenticate both party i.e. user and virtual machine. Kaman protocol is a protocol which authenticate both server node and user node and create mutual trust between both .Using this approach virtual side channel can be isolate from virtual side channel attacks.

Received March 13, 2015; Revised May 24, 2015; Accepted June 10, 2015

2. Background Study

Mazhar Ali, *et.al* (2015), discuss the various security issues in cloud computing and solution against security issues to counter them. A briefed discussion on security vulnerabilities is also given [8]. Vijay Varadharajan*, et.al* (2013), proposed a trust enhanced security model which helps to detect and prevent the security attacks in cloud using trusted attestation techniques [9].

Shikha Singh, *et.al* (2013), discussed the different attacks and their respective corresponding solutions. Through virtual side channel attack, how attacker can place the virtual machine to get into cloud is described. The two techniques virtual firewall appliance and randomly encryption decryption are proposed as a solution [10].

Abdulrahman Alumutairi, *et.al* (2014), proposed algorithm for risk aware cloud virtual resources assignment [11].

B. Clifford Neuman, et.al (1994), describes an authentication protocol which is used to authenticate users in distributed environment. Through Kerberos a user can authenticate itself to multiple servers using password. In this there is a KDC (key distribution centre) which contains authentication server (AS) and ticket granting server (TGS), application server (V) and a number of clients. Client receives ticket granting ticket (TGT) from AS, send this ticket to TGS to get service ticket and then send service ticket to V to get service [12, 15].

Asad Amir Pirzada*, et.al* (2004), describes Kaman protocol as authentication service for mobile and ad-hoc network. Kaman migrate a no. of features of Kerberos authenticated protocol. The main features includes preventing the forgery of node identity, detection of replay attacks, establishment of secure network, mutual authentication distribution of session keys among servers [13].

Heba Kandil, *et.al* (2014), proposed an architecture which is a software solution based on traditional Kerberos authentication system. The proposed architecture helps to prevent many mobile agent attacks and threats as it requires authenticating the mobile node to access any resources or service from server [14].

3. Virtual Side Channel Attack

In cloud computing, infrastructure service contains large no. of computer, virtual machines (VM), and other resources for their customers to store data, files and related information (Figure 1). It is possible to identify where a virtual machine is resides in cloud infrastructure [16, 17]. An attacker or intruder tries to compromise the cloud system by placing his own malicious virtual machine in place of target cloud server's virtual machine to get secret information and data related to users. Virtual side channel attack is performed by two steps:

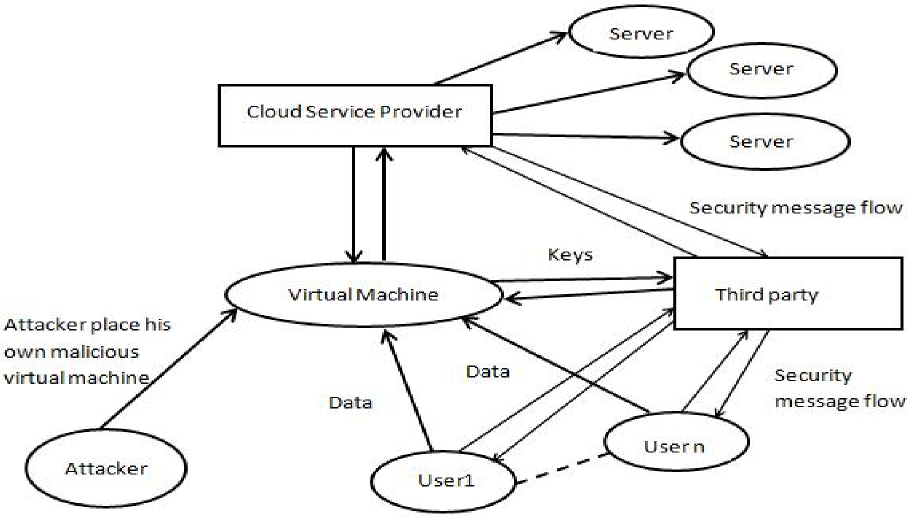

Figure 1. Virtual side channel attack

a) Virtual machine (VM) co-residence and Placement: an attacker places his own malicious instance on target instance.
b) Extraction: malicious virtual machine instance is used to get information about user and user's information.

Attacker forces users to give him all his credential like username and password. After getting credential of user attacker authorized on cloud as a valid user to get useful information of a user.

4. Proposed Protocol

Kaman- Kerberos assistant mobile ad-hoc network (KAMAN) protocol is an extension of the Kerberos protocol. Kaman protocol is used to authenticate the nodes in the ad-hoc network by secure server. Nodes are mutually authenticated. It is symmetric, key based authentication mechanism which involves both direct and indirect authentications. The main points in Kaman protocol are (Figure 2):

a) Password of user is hashed and store on server. Each user has his own password and only known to him.
b) Mutual authentication should be their between the servers. Servers share a secret key with each other for mutual authentication.
c) Servers shared a secret key. Repository is encrypted with secret key.

In Kerberos protocol three parties are involved: user, authenticated server and ticket granting server. A large no of messages are required to exchange for authentication and getting service from server. But in KAMAN protocol, two parties are involved: one is the client node and the other one is the authentication server thus lesser number of messages are required to transfer between node and server for authentication and starting service.

When a client wants to communicate with other client, then mutual authentication is required for both the client and server. Client send request to the server, client get authenticated and server send ticket to the client. Then client send that ticket to the another client and get acknowledged. Ticket has shared key which is created by server. By using this shared key data is encrypted and shared between two clients.

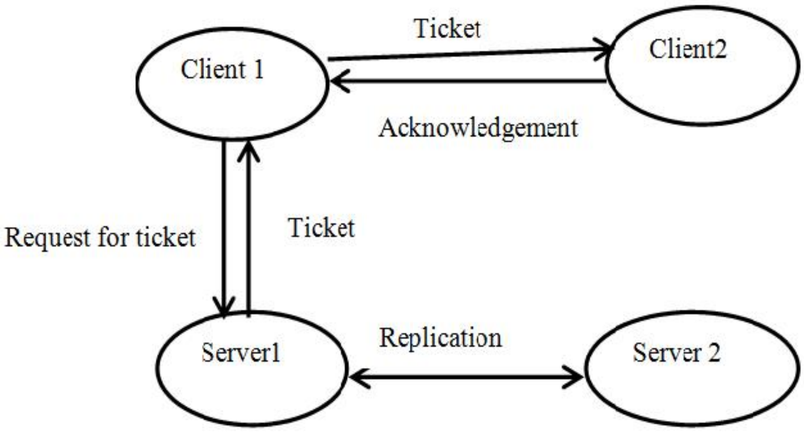

Figure 2. Working of Kaman protocol

There is also a replicated server and replica is produced from time to time to avoid single point of failure. Authentication server and replicated servers are also mutually authenticated. Election mechanism is used to select the secure server. When nodes are authenticated with the server, a session is established between the node and the server.

Client-Server-Client authentication procedure is shown in Table 1.

4.1. KAMAN Client-Server-Client Communication

Table 1. Client-Server-Client Authentication

Client1→Server Options, ID$_{C1}$, ID$_{C2}$, Times, Nonce
Server→ Client1 ID$_{C1}$, Ticket$_{C2}$,{K$_{C1,C2}$, Times, Nonce, ID$_{C2}$} K$_{C1}$
Client1→Client2 Options, Ticket$_{C2}$, Authenticator$_{C1}$
Client2→Client1 {TS, Subkey, Seq#} K$_{C1}$, K$_{C2}$ Ticket$_{C2}$={Flags, K$_{C1, C2}$, ID$_{C1}$, AD$_{C1}$, Times} K$_{C2}$ Authenticatior$_{C1}$={ID$_{C1}$, TS}K$_{C1,C2}$

Options- used to request that certain flags be set in the returned ticket.
Times - specify the start, end renew time setting in ticket.
Flags - ticket status.
Nonce -random value as identifier to avoid replay attacks.
Subkey - instead of using Kc1,c2 other encryption key for the session.
Seq# - starting seq. no. to detect replays attacks.
ID$_{C1}$ – Client1 identity
ID$_{C2}$ – Client2 identity
AD$_{C1}$ - Client1‘s network address.
K$_{C1}$- Encryption key of client1 based on the hashed value of the password
K$_{C1, C2}$ - Session key between client1 and client2.
TS - Time when authentication generated.

5. Research Methodolgy

As in cloud environment virtual side channel attack is possible. Attacker can compromise the identity of user and can access the user’s data and secret information on clouds. To prevent this side channel attacks Kaman protocol can be used to authenticate the virtual machine and users. Mutual authentication is established between virtual machines and users. When the identity of user and virtual machine is proven trust relationship is build. User and virtual machine can communicate and user can access and store the data on clouds. Figure 3 shows flow chart for proposed work.

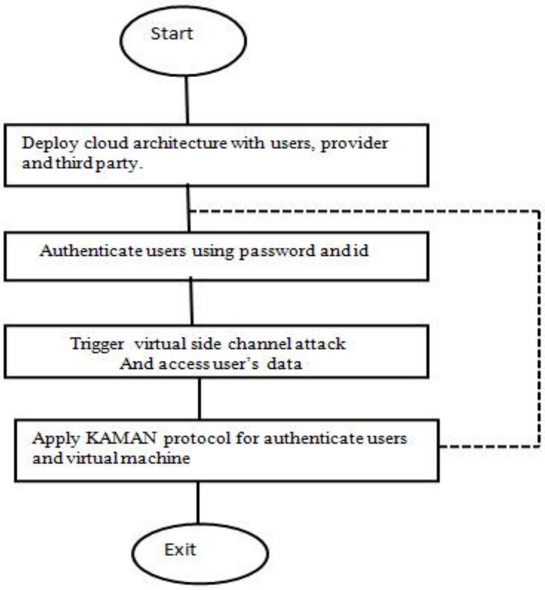
Start
Deploy cloud architecture with users, provider and third party.
Authenticate users using password and id
Trigger virtual side channel attack And access user’s data
Apply KAMAN protocol for authenticate users and virtual machine
Exit

Figure 3. Flow chart for proposed work

6. Result and Analysis

In this section, two scenarios are shown. In the first scenario, legitimate users authenticate to virtual machine and can store and retrieve their data through cloud service provider on virtual server. In the second scenario, Virtual side channel attack is triggered through an attacker is shown.

6.1. Legitimate User Authentication and Communication with Virtual Machine Scenario

In this scenario, Figure 4 shows nodes of network which are deployed. In our case 41 network nodes are deployed. In Figure 5 shows network of nodes where a fixed no. of users deployed with virtual machine cloud service provider and virtual servers are also shown where user's data is stored.

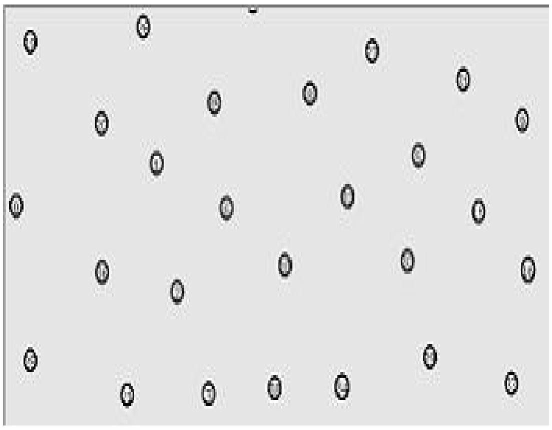

Figure 4. Deploying network nodes

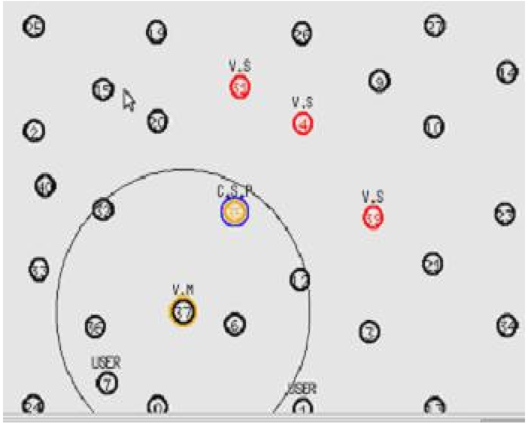

Figure 5. Deploying fix no. of user, virtual machine ,cloud service provider

In Figure 6, authentication of user is shown. User sends his id and password to virtual machine and authenticated as legitimate user. User starts communication through sending packets to the virtual machine. Through virtual machine user's data (Figure 7) is stored on virtual server through cloud.

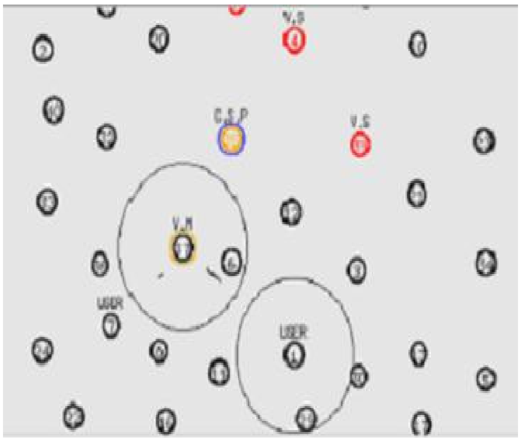

Figure 6. User authentication to virtual machine

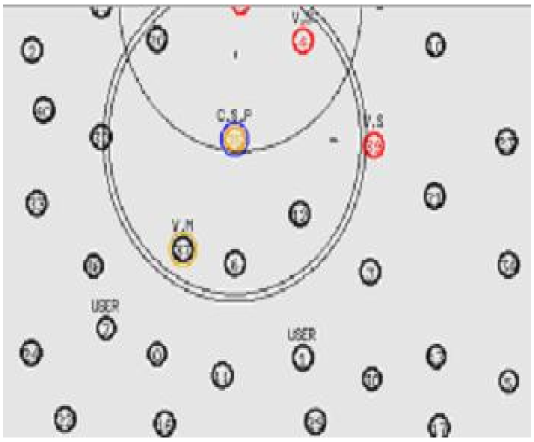

Figure 7. User data stored at virtual server through virtual machine and cloud service provider

6.2. Attacker Trigger Virtual Side Channel Attack and Extract User's Data Scenario

In the second scenario, attacker triggers the virtual side channel attack. Figure 8 shows, an attacker place his malicious virtual machine and hijack the credentials of user by spoofing technique. Figure 9 shows, attacker gets the credential of user and authenticate with the virtual machine through user's credentials as a legitimate user. Figure 10 shows finally attacker extract the user's information from virtual server through interacting with virtual machine.

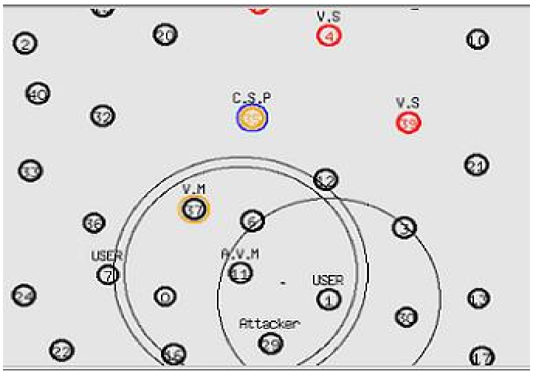

Figure 8. Attacker place his own virtual machine and stole credential of users

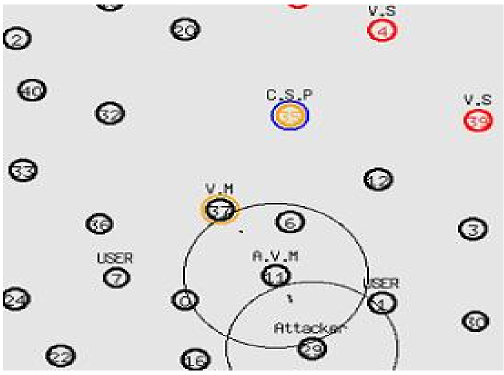

Figure 9. Attacker authenticate as legitimate user to virtual machine through user's credential

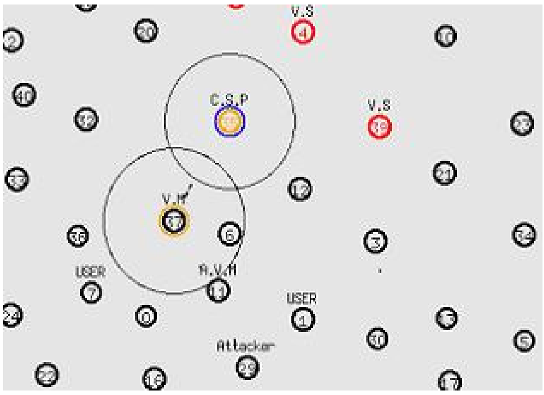

Figure 10. Attacker extract user's information from virtual server through virtual machine and cloud service provider

To isolate the virtual side channel attack, Kaman protocol is used to authenticate both the user and the virtual machine. A trust relationship is built between the user and virtual machine as to develop mutual trust. Before sending data to virtual machine user ask the credential of virtual machine and send his credential to virtual machine for authentication. Thus virtual side channel is isolated through using KAMAN protocol for authentication of users and virtual machine.

7. Conclusion

The Cloud computing has many security challenges that are exacerbated by virtual resource sharing. As virtual side channel is possible in cloud environment where an attacker place his virtual machine and break the confidentiality and privacy of user's data. Kaman protocol is one of the techniques which can be used to prevent the virtual side channel attacks in cloud environment.

References

[1] Diogo AB Fernandes, Liliana FB Soares, Joas V Gomas, Mario M Freire Pedro RM Inacio. S*ecurity issues in cloud environment: a survey*. Published online. Springer. 2013.

[2] A Prasad, et al. A mechanism design approach to resource procurement in cloud computing. *IEEE*. 2014; 63(1): 17-30.

[3] K Alhamazanni, R Ranjan, et al. *An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state of the art.* arXiv. 2014: 357-377.

[4] K Hashizume, et al. An analysis of security issues for cloud computing. *Journal internet services application*. 2013; 4(1): 1-13.

[5] Q Duan, Y Yan, et al. A survey on service oriented network virtualization toward convergence of networking and cloud computing*. IEEE trans. Netw. Service Manage.* 2012; 4(1): 373-392.

[6] Rabi Prasad Padht*,* et al*.* Evolution of cloud computing and enabling technologies*. IAES, IJ-CLOSER*. 2012; 1(4): 182-198.

[7] M Rajendra Prasad, et al*.* Cloud computing: research issues and implications. *IAES, IJ-CLOSER*. 2013; 2(2): 134-140.

[8] Mazhar Ali*,* et al*.* Security in cloud computing: opportunities and challenges*. Elsevier, Information sciences*. 2015; 305: 357-383.

[9] Vijay Varadharajan*,* et al*.* Counteracting security attacks in virtual machine in the cloud using property based attestation*. Journal of network and computer applications*. 2013; 40: 31-35.

[10] Shikha Singh, Binay Kumar pandey, et al*.* Cloud computing attacks: a discussion with solution. *Open journal of mobile computing and cloud computing*. 2013.

[11] Abdulrahman Almutairi, Arif Ghafoor. *Risk aware virtual resources management for access control-based cloud datacenters. C*erias tech report. 2014.

[12] B Clifford Neuman, Theodore ts'o. Kerberos: an authentication service for computer networks. *IEEE communication magazine*. 1994.

[13] Asad Amir Pirzada, Chris Mcdinald. Kerberos assisted authentication in mobile ad-hoc networks. Australian computer society, inc. 2004; 26.

[14] Heba Kandil, et al*.* Mobile agents' authentication using a proposed light Kerberos system. *Informatics and systems*. 2014.

[15] Amir Keshvari Ilkhichi*,* et al*.* Modeling Kerberos Authenticating protocol using colored petri net*. IAES, IJINS*. 2013; 2(5): 403-416.

[16] Bhrugu Seval. Security against side channel attack in cloud computing. *International journal of engineering and advanced technology* (*IJEAT*). 2012; 2.

[17] K Bilal*,* et al*.* Trends and challenges in cloud data centers*. IEEE cloud compute mag*. 2014; 1(1): 10-20.